The Belarus Cyber Attack – Addressing IT/OT Interdependence

Andrew Ginter, VP Industrial Security
Waterfall Security Solutions

February 10, 2022

Ukrainian conflict puts critical infrastructure at risk

Belarussian "cyber activists" disrupted passenger rail traffic in the country by encrypting ticketing and other IT systems. The activists demanded that the government stop hosting Russian troops and demanded the release of 50 political prisoners before the attackers would relinquish control of the encrypted servers. The group threatened to extend their control into safety-critical rail switching systems if their demands were not met. In such an eventuality, the group said that their objective would be to shut down trains, especially those carrying Russian troops, not to threaten human lives.

What does this mean for the world?

Governments have already warned that national critical infrastructures are likely to be targets of cyberattacks, and this is doubly true in times of physical conflict. In addition, some governments have cautioned that targeting critical infrastructures with cyber-attacks may constitute acts of war. Cyber acts of war, however, will have to get in line behind physical acts of war if the Russia/Ukraine conflict escalates into a physical conflict where Ukraine, Ukrainian allies, and NATO are in effect at war with Russia and her allies.

Keeping the lights on

The attack on the Belarusian rail system is yet another example of an attack that cripples IT systems, and so brings about OT consequences, like the Colonial Pipeline attack, and the JBS meatpacking attack. In this case the rail system attack brought about confusion, delayed passenger trains and cancellations, all because of crippled ticketing systems. As a rule, such physical consequences are unacceptable to societies and their governments when those consequences impair critical national infrastructures.

In the USA for example, shortly after the Colonial Pipeline attack caused widespread gasoline shortages, the TSA issued a new cybersecurity directive to the nation's largest pipelines. While initially secret, a redacted version of the directive was made available via the Washington Post, in response to a freedom of information request. Directive 2(b) of the document directs pipeline owners and operators to:

"Implement network segmentation sufficient to ensure the Operational Technology system can operate at necessary capacity even if the Information Technology system is compromised …"

This is the heart of the directive. Modern societies depend on critical infrastructures, and IT networks are intrinsically more exposed to Internet-based and other online attacks than OT networks should be. The government ordered pipeline operators to keep the pipeline going, even if IT assets have been breached. But it takes a number of things working together to keep a pipeline or power plant or rail system running while IT networks are crippled. The most important two are:

1. Network segmentation measures strong enough to prevent OT networks from being shut down "in an abundance of caution," when IT is compromised, and
2. Manual business processes or other contingencies able to compensate for crippled ticketing systems, billing systems, shipment tracking systems or other crippled IT resources.

Both these measures are necessary. It does no good having a pristine OT/ICS network if we must shut down operations because those operations rely on functionality in a crippled IT network. And it does no good having workarounds for crippled IT functions if the attack drifts or pivots from IT assets into the OT/ICS network and there forces a shutdown of physical operations.

Unidirectional technology can help

Unidirectional security gateways can help, especially with the directive to employ strong network segmentation. Unidirectional gateways are the strongest possible kind of IT/OT segmentation for OT networks. As defined by NIST SP 800-82 r2, the gateways are a combination of hardware and software. The hardware is physically able to send data out to the business network, and physically not able to send anything back into operations. It does not matter what kind of chaos has consumed the IT network, no online attacks, no matter how sophisticated – *nothing* – gets back into the operations networks through a unidirectional gateway.

Unidirectional gateway software makes copies of servers. The software logs into OT databases, historians, OPC servers, pub/subsystems, and other servers and asks for all the latest real-time data. The software converts the data into unidirectional protocols and pushes the data out to the IT network. On the IT network, the unidirectional gateway software receives the data and then inserts it into an identical server. IT users and applications log into and use the replica database, historian, OPC, pub/sub, etc. servers normally. Unidirectional software makes deployment of the unidirectional hardware painless and seamless.

Difficult times

These are difficult times. The incident in Belarus is very likely only the first of many incidents targeting critical national infrastructures. If the crisis worsens, we should expect many more such incidents targeting infrastructures in NATO nations and in any other nations that support either Russia or Ukraine. And bear in mind – while the incident in Belarus was hacktivists, Russia is a cyber superpower. Russia has the means to bring *very* sophisticated attacks to bear on critical infrastructure targets – this was the point of the recent DHS warnings in the United States.

And it is a mistake to think that these threat actors will target only large and heavily-defended critical infrastructures – smaller, "less important" and *less defended* infrastructures will be very attractive targets as well.

The good news – deploying unidirectional gateways can be very straightforward. There are a variety of unidirectional products on the market that most often are "set and forget" – unlike IT/OT firewalls, there is no constant fiddling or monitoring needed for unidirectional products. Even better, some unidirectional products are configured and managed and, if necessary, diagnosed and repaired with simple, thin-client, web tools.

The time has come to make our OT/ICS networks essentially impenetrable to online hacktivist, ransomware and nation-state attacks. We need to do this before we are targeted and before we suffer consequences as part of this Russia/Ukraine crisis, or as part of any of the other geopolitical crises that await in the months ahead.

To learn more about unidirectional protection for critical infrastructure, especially rail systems, please download Waterfall's latest rails cybersecurity report.

# # #